problem not easily overcome. What we can overcome, however, are the gaps, the weaknesses, the outdated strategies, and the inadequate resources in our own legal investigative processes.

One example: the most dangerous cyber criminals are usually located overseas. To identify, investigate, and ultimately prosecute those criminals under traditional law enforcement authorities, we have to rely on complex and cumbersome international processes and treaties established decades ago that are far too slow for the modern cyber crime environment.

We also need to resource and focus criminal investigation and prosecution at a level commensurate with the fact that we, America, are now on the losing end of what is probably the biggest transfer of wealth through theft and piracy in human history.

I will say that again: We are at the losing end of what is probably the biggest transfer of wealth through theft and piracy in human history.

I am pleased that in fiscal year 2010 the FBI received an additional 260 cyber security analysis and investigative positions. DOJ's Computer Crimes and Intellectual Property Section has not received new resources in 5 years. With the FBI poised to ramp up its investigatory actions against our cyber adversaries, I am concerned the DOJ may not have the resources to keep up.

Sixth, we need clear rules of engagement for our government to deal with foreign threats. That is, unfortunately, a discussion for another day since so much of this area is now deeply classified. But here is one example: Can we adapt traditional doctrines of deterrence to cyber attacks when we may not know for sure which country or nonstate actor carried out the attack? If we can't attribute, how can we deter?

With respect to any policy of deterrence, how can it stand on rules of engagement that the attacker does not know of? Not only do we need to establish clear rules of engagement, we need to establish and disclose clear rules of engagement if any policy of deterrence is to be effective in cyberspace.

Finally, as we go about these six tasks, the government must be as transparent as possible with the American people. I doubt very much that the Obama administration would abuse new authorities in cyberspace to violate Americans' civil liberties. But on principle, I firmly and strongly believe that maximum transparency to the public and rigorous congressional oversight are essential. We have to go about this right.

I look forward to working with my Senate colleagues and with the administration as the Congress moves toward comprehensive cyber security legislation to protect our country before a great cyber attack should befall us.

Let me close my remarks by saying the most somber question we need to face is resilience.

First, resilience of governance: How could we maintain command and control, run 9–1–1, operate FEMA, deploy local police and fire services, and activate and direct the National Guard if all of our systems are down?

Second, resilience of society: How do we make sure people have confidence during a prolonged attack that food, water, warmth, and shelter will remain available? Because the Internet supports so many interdependent systems, a massive or prolonged attack could cascade across sectors, compromising or taking over our communications systems, our financial systems, our utility grid, and the transportation and delivery of the basic necessities of American life.

Third, our American resilience as individuals: Think about it. Your power is out and has been for a week. Your phone is silent. Your laptop is dark. You have no access to your bank account. No store is accepting credit cards. Indeed, the corner store has closed its doors and the owner is sitting inside with a shotgun to protect against looters. Gasoline supply is rationed with National Guard soldiers keeping order at the pumps. Your children are cold and hungry and scared. How, then, do you behave?

I leave this last question, our resilience as a government, as a society, and as individuals to another day. But I mention it to highlight the potentially catastrophic nature of a concerted and prolonged cyber attack. Again, such an attack could cascade across multiple sectors and could interrupt all of the different necessities on which we rely.

When your power is down, it is an inconvenience but you can usually call somebody on the phone. Now the phone is out, so you can go to the laptop and try to e-mail somebody, but there is no signal on the laptop. You need cash. You go to the ATM. It is down. The bank is not open because a run would take place against its cash assets, given the fact that it can no longer reliably electronically let its customers know what their bank account balances are.

We are up against a very significant threat. I hope some of the guideposts I have laid out will be helpful in designing the necessary legislation we need to put in place to empower our country to successfully defend against these sorts of attacks.

I yield the floor. I suggest the absence of a quorum.

The PRESIDING OFFICER. The clerk will call the roll.

The assistant editor of the Daily Digest called the roll.

Mr. WHITEHOUSE. Mr. President, I ask unanimous consent that the order for the quorum call be rescinded.

The PRESIDING OFFICER. Without objection, it is so ordered.

MORNING BUSINESS

Mr. WHITEHOUSE. Mr. President, I ask unanimous consent that the Senate proceed to a period of morning business, with Senators permitted to speak for up to 10 minutes each.

The PRESIDING OFFICER. Without objection, it is so ordered.

TRIBUTE TO ROBERT FORBUSS

Mr. REID. Mr. President, I rise today to honor Mr. Robert ''Bob'' Forbuss for his service to the people of Nevada. Tomorrow evening, at its Annual Convention and Tradeshow in Las Vegas, the American Ambulance Association will honor Mr. Forbuss for his many years of work on behalf of ambulance services in Nevada and throughout the Nation. Today I am happy to call the attention of the Senate to the selfless service that my good friend has rendered to the State of Nevada.

Bob is a native Nevadan who has served this community for nearly four decades as an educator, elected official, businessman, and community advocate. After earning his degrees in political science and public administration from Long Beach State University, Bob returned to Las Vegas and began his professional career as a teacher at Bishop Gorman High School from 1972–1979. He then served on the Clark County School Board of Trustees for 8 years and was an influential advocate for education initiatives in Southern Nevada. For his many years of service to education in Nevada, Bob was eventually honored by the Clark County School District in the naming of the Robert L. Forbuss Elementary School. It is fitting that such a fine educator will forever have his name stamped on the hearts of the students that attend Forbuss Elementary School.

During his tenure at Bishop Gorman, Bob became an emergency medical technician, EMT, and worked during his summer breaks for Mercy Medical Services. He quickly worked his way through the managerial ranks of Mercy and eventually became an owner of the company. Mercy soon became a flagship and model operation in the United States for paramedic services and Bob became a recognized leader in EMS Services, winning numerous awards and becoming a popular speaker at national conferences.

One of his greatest achievements, and the one for which he is being recognized tomorrow evening, has been his work on behalf of the American Ambulance Association, AAA. The AAA was formed in response to the need for improvements in medical transportation and emergency medical services. Bob was an original founder of the AAA, and he later served as the organization's president. I have no doubt that throughout his presidency, and the subsequent years of service that followed, he has labored diligently to ensure that our Nation's ambulatory systems have the resources they need to serve our families, friends, and communities.

Today, I express my sincere thanks to my dear friend for the noble work that he has performed over the years.